IN THE CLAIMS

Please amend the claims as follows:

Claims 1-31 (Canceled).

Claim 32 (New): A denial-of-service attack protecting method of protecting a communication device against a denial of service attack using a gate device connected to the communication device or a repeater device connected to the gate device and that is a part of a network, comprising:

an authorized device on the network issuing authorized address information indicative of a source address of a non-attacking packet; and

the gate device controlling passage of a packet on the network based on the authorized address information.

Claim 33 (New): The denial-of-service attack protecting method according to claim 32, further comprising:

the gate device receiving the authorized address information from the authorized device;

the gate device generating normal condition information indicative of conditions for the non-attacking packet based on the authorized address information; and

the gate device allowing passage of a packet that satisfies the conditions in the normal condition information.

Claim 34 (New): The denial-of-service attack protecting method according to claim 33, wherein the gate device receiving the authorized address information includes

the gate device first reporting own address information to the repeater device;

upon receiving authorized address information from the authorized device, the repeater device relaying received authorized address information to the gate device based on the address information reported in the first reporting; and

the gate device receiving the authorized address information from the repeater device.

Claim 35 (New): The denial-of-service attack protecting method according to claim 34, wherein the first reporting includes

the repeater device, to which the gate device has reported own address information, relaying the address information to a second repeater device that is provided adjacent to the repeater device; and

upon receiving authorized address information from the authorized device, the second repeater device relaying the authorized address information to any one of a third repeater device adjacent to the second repeater device and the gate device based on the address information.

Claim 36 (New): The denial-of-service attack protecting method according to claim 33, wherein the gate device receiving the authorized address information includes

an authorized address information providing device, which integrally manages authorized address information, receiving the authorized address information from the authorized device, and storing the received authorized address information;

when accepting a transmission request for the authorized address information from the gate device, the authorized address information providing device reporting to the gate device the authorized address information requested for its transmission; and

the gate device receiving the authorized address information.

Claim 37 (New): The denial-of-service attack protecting method according to claim 33, wherein gate device receiving the authorized address information includes

the gate device receiving the authorized address information transmitted by any one of an address issuing device that issues an address and a communication device that is authorized.

Claim 38 (New): The denial-of-service attack protecting method according to claim 33, further comprising:

the gate device detecting an attack performed by an attacking packet received via the network;

the gate device generating a suspicious signature indicative of a feature of the attacking packet;

the gate device storing the normal condition information in a normal condition information storage unit; and

the gate device generating a normal signature indicative of a feature of a packet, which satisfies the conditions in the normal condition information, among packets applying to the suspicious signature, wherein

the gate device allowing passage based on the suspicious signature and the normal signature.

Claim 39 (New): The denial-of-service attack protecting method according to claim 38, further comprising:

the gate device reporting the suspicious signature and the normal signature to the repeater device; and

the repeater device controlling passage of a packet based on the suspicious signature and the normal signature.

Claim 40 (New): The denial-of-service attack protecting method according to claim 32, further comprising:

the gate device detecting an attack performed by the attacking packet received via the network;

upon the gate device detecting the attack, the gate device receiving authorized address information from the repeater device, the authorized address information indicative of a source address of a non-attacking packet which is received from an authorized device on the network; and

the gate device controlling passage of a packet based on normal condition information indicative of conditions for the non-attacking packet, wherein the normal condition information is generated from the authorized address information received from the repeater device.

Claim 41 (New): The denial-of-service attack protecting method according to claim 40, further comprising the gate device generating a suspicious signature indicative of a feature of the attacking packet, wherein the gate device receiving authorized address information includes

the gate device transmitting the suspicious signature to the repeater device, and receiving authorized address information returned in response from the repeater device.

Claim 42 (New): The denial-of-service attack protecting method according to claim 41, wherein the gate device controlling passage of a packet includes

generating normal condition information indicative of conditions for a non-attacking packet based on received authorized address information; and

the gate device restricting passage of an attacking packet while allowing passage of a non-attacking packet that matches the conditions in the normal condition information among packets received from the network.

Claim 43 (New): The denial-of-service attack protecting method according to claim 42, further comprising generating a normal signature indicative of a feature of a packet that matches conditions in the normal condition information, wherein

the gate device controls passage of a packet based on the suspicious signature and the normal signature.

Claim 44 (New): The denial-of-service attack protecting method according to claim 43, further comprising the gate device forwarding the normal signature to the repeater device.

Claim 45 (New): A denial-of-service attack protecting system that protects a communication device against a denial of service attack using a gate device connected to the communication device or a repeater device connected to the gate device and that is a part of a network, wherein the gate device comprises:

an authorized address information acquiring unit that acquires authorized address information indicative of a source address of a non-attacking packet transmitted by an authorized device on the network;

a normal condition information generating unit that generates normal condition information indicative of conditions for the non-attacking packet, based on the authorized address information acquired by the authorized address information acquiring unit; and

a packet controlling unit that controls passage of packets on the network, wherein the packet controlling unit restricts passage of an attacking packet that do not satisfy the conditions in the normal condition information while allowing passage of a non-attacking packet that satisfies the conditions in the normal condition information.

Claim 46 (New): A denial-of-service attack protecting system that protects a communication device against a denial of service attack using a gate device connected to the communication device or a repeater device connected to the gate device and that is a part of a network, wherein the gate device comprises:

an attack detecting unit that detects an attack on the communication device by an attacking packet;

an authorized address information receiving unit that, upon the gate device detecting the attack, receives authorized address information from the repeater device, the authorized address information indicative of a source address of a non-attacking packet which is received from an authorized device on the network; and

a passage controlling unit that controls passage of a packet based on normal condition information indicative of conditions for the non-attacking packet, wherein the normal condition information is generated from the authorized address information received by the authorized address information receiving unit.

Claim 47 (New): A gate device that protects a communication device against a denial of service attack, the gate device being connected to the communication device or a repeater device connected to the gate device and that is a part of a network, comprising:

an authorized address information acquiring unit that acquires authorized address information indicative of a source address of a non-attacking packet transmitted by an authorized device on the network;

a normal condition information generating unit that generates normal condition information indicative of conditions for the non-attacking packet, based on the authorized address information acquired by the authorized address information acquiring unit; and

a packet controlling unit that controls passage of packets on the network, wherein the packet controlling unit restricts passage of an attacking packet that do not satisfy the conditions in the normal condition information while allowing passage of a non-attacking packet that satisfies the conditions in the normal condition information.

Claim 48 (New): The gate device according to claim 47, wherein the authorized address information acquiring unit includes

an address information reporting unit that reports own address information to the repeater device; and

a receiving unit that receives the authorized address information from the authorized device sent back by the repeater device in response to the address information for the own device reported by the address information reporting unit.

Claim 49 (New): The gate device according to claim 48, wherein the authorized address information acquiring unit includes

an authorized address information transmission requesting unit that issues a transmission request for the authorized address information to an authorized address information providing device that integrally manages authorized address information; and

a receiving unit that receives the authorized address information sent back in response to the transmission request for the authorized address information.

Claim 50 (New): A gate device that protects a communication device against a denial of service attack, the gate device being connected to the communication device or a repeater device connected to the gate device and that is a part of a network, comprising:

an attack detecting unit that detects an attack on the communication device by the attacking packet;

an authorized address information receiving unit that, upon the gate device detecting the attack, receives authorized address information from the repeater device, the authorized address information indicative of a source address of a non-attacking packet which is received from an authorized device on the network; and

a passage controlling unit that controls passage of a packet based on normal condition information indicative of conditions for the non-attacking packet, wherein the normal condition information is generated from the authorized address information received by the authorized address information receiving unit.

Claim 51 (New): The gate device according to claim 50, further comprising a suspicious signature generating unit that generates a suspicious signature indicative of a feature of the attacking packet, wherein

the authorized address information acquiring unit transmits the suspicious signature to the repeater device, and receives authorized address information returned in response from the repeater device.

Claim 52 (New): The gate device according to claim 51, wherein the passage controlling unit includes

a normal condition information generating unit that generates normal condition information indicative of conditions for a non-attacking packet based on received authorized address information; and

a packet restricting unit that restricts passage of an attacking packet while allowing passage of a non-attacking packet that matches the conditions in the normal condition information.

Claim 53 (New): A repeater device connected to a gate device that protects a communication device being a target of a denial of service attack, and/or connected to one or more repeater devices that form a network, comprising:

an address information acquiring unit that acquires address information for the gate device; and

an authorized address information relaying unit that relays authorized address information to any one of the gate device and a second repeater device adjacent to the repeater device based on the address information acquired by the address information acquiring unit, when receiving the authorized address information indicating a source address of a non-attacking packet transmitted by an authorized device on the network.

Claim 54 (New): A repeater device connected to a gate device that protects a communication device being a target of a denial of service attack, and/or connected to one or more repeater devices that form a network, comprising:

an authorized address information storage unit that stores authorized address information indicative of a source address of a non-attacking packet received from an authorized device on the network; and

a transfer unit that transfers the authorized address information stored in the authorized address information storage unit to a gate device when the gate device detects an attack on the communication device.

Claim 55 (New): A computer-readable recording medium that stores therein a computer program that causes a gate device to protect a communication device against a denial of service attack, the gate device being connected to the communication device or a repeater device connected to the gate device and that is a part of a network, the computer program causing the gate device to execute:

acquiring authorized address information indicative of a source address of a non-attacking packet transmitted by an authorized device on the network;

generating normal condition information indicative of conditions for the non-attacking packet, based on the authorized address information acquired by the authorized address information acquiring unit; and

controlling passage of packets on the network, wherein the packet controlling unit restricts passage of an attacking packet that do not satisfy the conditions in the normal condition information while allowing passage of a non-attacking packet that satisfies the conditions in the normal condition information.

Claim 56 (New): The computer-readable recording medium according to claim 55, wherein the acquiring includes

reporting own address information to the repeater device; and

receiving the authorized address information from the authorized device sent back by the repeater device in response to the address information for the own device reported by the address information reporting unit.

Claim 57 (New): The computer-readable recording medium according to claim 55, wherein the acquiring includes

issuing a transmission request for the authorized address information to an authorized address information providing device that integrally manages authorized address information; and

receiving the authorized address information sent back in response to the transmission request for the authorized address information.

Claim 58 (New): A computer-readable recording medium that stores therein a computer program that causes a gate device to protect a communication device against a denial of service attack, the gate device being connected to the communication device or a repeater device connected to the gate device and that is a part of a network, the computer program causing the gate device to execute:

detecting detects an attack on the communication device by the attacking packet;

receiving, upon detecting the attack at the detecting, authorized address information from the repeater device, the authorized address information indicative of a source address of a non-attacking packet which is received from an authorized device on the network; and

controlling passage of a packet based on normal condition information indicative of conditions for the non-attacking packet, wherein the normal condition information is generated from the authorized address information received by the authorized address information receiving unit.

Claim 59 (New): The computer-readable recording medium according to claim 58, wherein the computer program further causes the gate device to generating a suspicious signature indicative of a feature of the attacking packet, wherein

the receiving includes transmitting the suspicious signature to the repeater device, and receiving authorized address information returned in response from the repeater device.

Claim 60 (New): The computer-readable recording medium according to claim 59, wherein the controlling includes

generating normal condition information indicative of conditions for a non-attacking packet based on received authorized address information; and

restricting passage of an attacking packet while allowing passage of a non-attacking packet that matches the conditions in the normal condition information.

Claim 61 (New): A computer-readable recording medium that stores therein a computer program that causes a repeater device connected to a gate device to protect a communication device being a target of a denial of service attack, and/or connected to one or more repeater devices that form a network, the computer program causing the repeater device to execute:

acquiring address information for the gate device; and

relaying authorized address information to any one of the gate device and a second repeater device adjacent to the repeater device based on the address information acquired by the address information acquiring unit, when receiving the authorized address information indicating a source address of a non-attacking packet transmitted by an authorized device on the network.

Claim 62 (New): A computer-readable recording medium that stores therein a computer program that causes a repeater device connected to a gate device to protect a communication device being a target of a denial of service attack, and/or connected to one or more repeater devices that form a network, the computer program causing the repeater device to execute:

storing authorized address information indicative of a source address of a non-attacking packet received from an authorized device on the network; and

transferring stored authorized address information to a gate device when the gate device detects an attack on the communication device.